基于安全信任的网络切片部署策略研究*

牛　犇，游　伟，汤红波

(国家数字交换系统工程技术研究中心，郑州 450002)

摘　要：5G 移动通信网虚拟化场景下，如何安全部署网络切片是未来 5G 大规模商用的前提。针对 5G 网络切片部署的安全性，提出一种基于安全信任的网络切片部署策略。该部署策略通过提出安全信任值概念，来有效量化分析 VNF 和网络资源的安全性，并以此为基础，利用 0-1 整数线性规划方法构建网络切片部署的数学模型，利用启发式算法进行求解，找到网络切片部署成本最小的部署方案。仿真实验表明，该部署策略在保证部署安全的前提下，减少了部署成本，同时获得较好的安全收益和部署收益率。

关键词：5G；网络切片；安全信任；部署

中图分类号：TN915.81　　doi: 10.3969/j.issn.1001-3695.2017.08.0728

Research on network slicing deployment strategy based on security trust

Niu Ben, You Wei, Tang Hongbo

(*National Digital Switching System Engineering & Technological R&D Center*, *Zhengzhou* 450002, *China*)

Abstract: In the 5G mobile communication network virtualization scenario, how to deploy network slices safely is a prerequisite for future large-scale commercial use. Aiming at the security of 5G network slice deployment, this paper proposed a strategy for network slicing deployment based on security trust. The deployment strategy could effectively quantify and analyzed the security of VNF and network resources by proposing the concept of security trust value, and on this basis, constructed the mathematical model of network slice deployment using 0-1 integer linear programming method. The strategy used heuristic algorithm to find the minimum cost of network slice deployment. Simulation results show that the deployment strategy reduces the deployment cost and achieves better security revenue and deployment rate of return under the premise of ensuring the deployment security.

Key Words: 5G; network slicing; security trust; deployment

0　引言

随着物联网、车联网、工业控制以及垂直行业的兴起与发展，第五代移动通信（5G）技术将在多领域、多场景下满足用户定制化移动业务需求，实现“万物互联”的愿景[1]。5G 网络切片作为 5G 网络的关键技术，是在虚拟化技术的基础上，将多个虚拟网络功能（virtual network function, VNF）进行动态裁剪、编排并部署，形成相互独立的虚拟网络，每个虚拟网络可根据用户需求提供定制化的网络服务[2]。在 5G 架构下，网络切片部署能够有效增强网络的灵活性和弹性，促进基础设施资源的高效利用，大幅降低资本支出和运营成本，同时满足用户定制化的安全和服务需求，实现按需组网。

未来 5G 网络将采用软件定义网络(software defined network, SDN)和网络功能虚拟化(network function virtualization, NFV)技术，导致网络切片部署由于引进虚拟化技术而产生安全问题。在底层资源上部署网络切片时，可能存在一系列安全问题，例如受安全威胁的底层网络攻击虚拟网络（如嗅探攻击、恶意修改虚拟机信息等），受攻击的虚拟机影响 VNF 正常运行（如 DOS 攻击等），由于共享底层资源导致虚拟网络之间相互攻击（如跨虚拟机旁路攻击、侧信道攻击等）或者由于 VNF 软件中的安全漏洞而导致安全威胁等[3,4]。这些安全问题导致网络切片无法正常工作，破坏了网络切片的机密性和完整性；同时网络切片的安全性难以满足用户需求，阻碍了 5G 网络切片的大规模的部署和商用。因此，亟待新的安全机制和部署方法来满足网络切片部署的安全性。

网络切片部署难点主要是对切片中 VNF 进行部署，现有文献针对 VNF 部署问题，主要在互联网或演进分组核心网(evolved packet core, EPC)等网络场景和架构下，根据不同优化目标设计 VNF 部署策略，例如通过业务流量感知和节点分割算法对 vEPC 网络中池组化虚拟网络功能进行部署，可有效降低虚拟网络资源开销，提高网络接受率[5]；针对移动核心网网元（PGW、SGW、MME 等）形成的服务功能链(service function

基金项目：国家重点研发计划项目（2016YFB0801605）

作者简介：牛犇（1992-），男，内蒙古呼和浩特人，硕士研究生，主要研究方向为 5G 网络安全，网络功能虚拟化（18810388449@163.com）；游伟（1984-），男，讲师，博士，主要研究方向为密码学及 5G 网络安全；汤红波（1968-），男，教授，博导，主要研究方向为移动通信网络、新型网络体系结构.

chain, SFC)进行网元功能部署和网络拓扑优化[6]；利用遗传算法对 VNF 进行动态部署，有效解决由于动态请求或请求变更而导致的 VNF 静态部署不适应的问题[7]；通过设计多种遗传算法，对链路最大利用率以及带宽消耗进行优化[8]；利用近似优化算法部署 VNF[9]；利用整数线性规划和启发式算法对 SFC 进行部署[10]；建立部署模型对 SFC 进行部署和评价[11]；针对 SFC 的大规模部署问题，将变邻域搜索和元启发式算法相结合，能够找到可行的设计方案[12]；针对运营成本设计一种弹性的 VNF 部署策略[13]。综上所述，目前 VNF 部署策略，主要以降低 VNF 部署成本，提高资源利用率和平衡网络拓扑负载等作为优化目标进行设计，针对 VNF 安全尤其是在 5G 网络架构下的 VNF 部署安全可参考的文献和方法较少，因此本文提出一种网络切片安全部署算法，以应对网络切片部署时的安全性需求。

针对上述网络切片安全部署方法的不足，本文利用 0-1 整数线性规划方法建立数学模型，以最小部署成本作为部署目标，提出一种基于安全信任的网络切片部署策略。在部署过程中利用安全信任值来有效量化分析 VNF 和网络资源的安全性，通过对 VNF 安全等级进行排序，实现在部署中将高安全等级的 VNF 进行优先部署和重点保护。仿真实验表明，该部署策略通过考虑全局的资源和安全属性，所获得的部署方案在保证安全的前提下，在部署成本，安全收益和部署收益率等方面都获得良好的性能。

1　问题描述与数学模型

1.1　安全部署问题描述

5G 网络在 SDN/NVF 技术的基础上，网络功能与原有 EPC 架构中的网元功能相区分，网络功能细粒度化，提高了网络的灵活性；同时将原本价格昂贵的专属硬件设备以软件化形式迁移到通用的服务器上，大大降低了运维成本。经过 SDN 控制器统一编排后的网络切片，在对其进行部署后，能组成一套完整的虚拟网络为用户提供业务服务[14,15]。

对网络切片进行部署时，根据 VNF 和请求链路的需求，在底层通用资源上进行部署进而实现用户所需的网络服务[16]。图 1 为网络切片部署示意图。本文在不是一般性的前提下，为了简化求解的复杂度，有效屏蔽复杂的物理底层细节，将实际部署中通用的物理硬件设备资源和通用的分布式云平台虚拟网络资源统一抽象为图 1 模型中的网络资源。

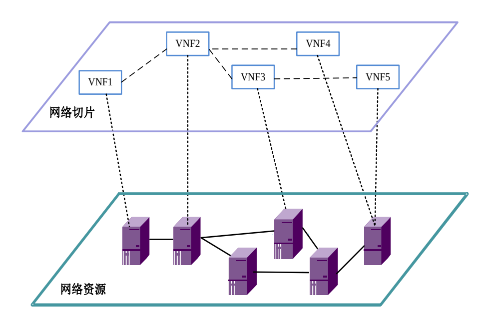


图 1　VNF 部署模型示意图

信任概念源于社会科学的人际关系网络，后被引入计算机科学中，信任安全作为网络安全中的“软安全”技术相较于传统安全技术（如加密技术、防火墙）具有更高的灵活性以及前瞻性[17]。为保证网络切片部署的安全性，本文提出安全信任值来量化网络资源和 VNF 的安全可信程度[18]。安全信任值在 0~1 之间，值越大，表明越安全可信。网络资源在具有越安全的资源链接管理、越高水平的安全映射机制、越多的安全保护机制等安全条件下，其安全信任值就越高；VNF 的安全信任值与其软件的编写水平相关（漏洞、后门出现的可能性越小，安全信任值就越高）。

图 2 为简化的 VNF 安全部署示例，左侧为 VNF 部署请求，(x, y, z) 分别表示 VNF 的 CPU 资源请求，VNF 对网络资源的安全信任值需求，VNF 自身的安全信任值；右侧为网络资源拓扑，(x, y, z) 分别代表网络资源节点可提供的 CPU 资源能力，资源节点的安全信任需求和其相应的安全信任值。根据图 3 描述，对于一个网络切片的部署请求，其在网络资源拓扑上的部署方案为 $\{VNF1 \rightarrow E, VNF2 \rightarrow B, VNF3 \rightarrow G\}$。

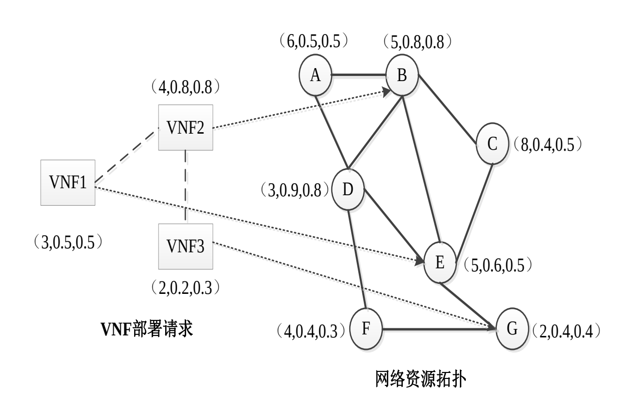


图 2　VNF 安全部署示例

为保证 VNF 部署的安全性，在部署时应满足以下安全约束条件：

a)网络资源节点的安全信任值不能低于部署在其上的 VNF 安全信任值需求，防止 VNF 部署在安全性较低的资源节点上；

b)VNF 自身的安全信任值不能低于部属在其上的网络资源节点的安全信任需求，防止 VNF 可能携带的安全漏洞影响网络资源的安全性；

c)在已部署 VNF 的网络资源节点上部署新的 VNF，新 VNF 自身的安全信任值不得低于已部署 VNF 的安全信任值，防止不安全的 VNF 利用共享的网络资源对其他 VNF 进行攻击；

d)对安全等级最高的 VNF 进行优先部署，同时不共享底层网络资源节点。

安全约束条件 a)~c)是保证 VNF 被安全的部署在底层网络资源的节点上，安全约束条件 d)是保证安全等级高的 VNF 不受同驻攻击的影响，降低安全风险，实现对高安全等级 VNF 的重点保护。

1.2　数学模型

网络资源表示为一个由网络节点和节点间链路组成的无向

图 $G^P=(N^P,E^P)$，其中 N^P 和 E^P 分别代表网络资源中的节点和链路集合。对于网络资源节点 $n_i^P\in N^P$，$n_i^P=(C_i^P,M_i^P,R_i^P,S_i^P)$，$C_i^P$、$M_i^P$、$R_i^P$ 和 S_i^P 分别表示底层资源节点 n_i^P 上的 CPU 资源能力值，存储能力值，资源节点的安全信任需求和资源节点的安全信任值；e_{ij}^P（$e_{ij}^P\in E^P$）表示为网络资源节点 n_i^P 和 n_j^P 之间的网络资源链路，$e_{ij}^P=(S_{ij}^P,B_{ij}^P)$ 其中 S_{ij}^P 表示为网络资源链路 e_{ij}^P 的安全性，S_{ij}^P 由节点 n_i^P 到节点 n_j^P 之间经过节点的最低安全信任值所决定，B_{ij}^P 表示为网络资源链路 e_{ij}^P 的所具有的带宽资源。$Hop(e_{ij}^P)$ 表示网络资源链路 e_{lv}^P 经过节点的跳数

网络切片的部署请求拓扑图由无向图 $Q^V=(F^V,E^V)$ 来表示，F^V 为所需部署的 VNF 集合，E^V 为请求链路集合。对于一个 VNF $f_i^V\in F^V$，$f_i^V=(C_i^V,M_i^V,R_i^V,S_i^V)$，其中 C_i^V、M_i^V、R_i^V 和 S_i^V 分别表示 f_i^V 的 CPU 资源需求值，存储资源需求值，VNF 对网络资源的安全信任需求以及 VNF 自身的安全信任值；对于拓扑图中的虚拟网络请求链路 e_{st}^V（$e_{st}^V\in E^V$）表示 f_s^V 和 f_t^V 之间的虚拟网络链路，$e_{st}^V=(B_{st}^V,R_{st}^V)$ 其中 B_{st}^V 表示链路 e_{st}^V 的带宽资源需求，R_{st}^V 表示链路 e_{st}^V 所需要的安全信任值。$f_{i,j}^V$ 表示 f_i^V 部署在底层网络资源节点 n_j^P 上，$e_{st,lv}^V$ 表示请求链路 e_{st}^V 部署在底层网络资源链路 e_{lv}^P 上。

2 VNF 安全等级研究

网络切片部署时，针对网络切片不同的应用场景，不同的用户需求，不同的业务范围和不同的风险因素，网络切片中的 VNF 应具有不同的安全等级。对高安全等级的 VNF 进行重点保护，可以有效提升网络切片整体的安全性；反之，攻击者对高安全等级的 VNF 进行攻击，会达到事半功倍的效果，体现出高安全等级 VNF 的脆弱性和易攻击性。因此针对 VNF 安全等级研究，对提高整个网络切片部署的安全性有着重要的作用。本章提出多种安全等级评价指标，通过 TOPSIS 分析法对 VNF 的安全等级进行合理排序。

2.1 安全等级评价指标

指标 1 根据 VNF 类型。图 3 是 3GPP 提出的基于服务 5G 网络架构，通过 SDN 技术将控制与承载分离，使得组成网络切片的 VNF 可分为控制平面 VNF 和用户平面 VNF。控制平面 VNF 负责会话管理、移动性管理、认证授权、协议管理等控制功能，用户平面 VNF（UPF 为用户平面功能集合）负责相对简单的路由转发功能。该评价指标计算时，将控制平面 VNF 安全等级指标设定为 1，用户平面 VNF 安全等级指标设定为 0。

指标 2 根据与 VNF 相连的所有邻接链路的通信量需求和。用 T_i 表示流经 f_i^V 的通信量，如式(1)所示。

$$T_i=T_i^{in}+T_i^{out} \tag{1}$$

流量指标 T_i 由 VNF 流入和流出的通信量决定。不同场景和业务下的网络切片，不同 VNF 的通信量需求有所不同。例如在 mMTC 场景下，大量物联网设备接入切片，切片中具有认证功能的 VNF 通信量需求较大；而在 eMBB 场景下，具有传输功能的 VNF 通信量需求较大；在自动驾驶的网络切片中，具有移动性管理功能的 VNF，其数据通信量需求将会较大。由于 5G 开放性的特点，频繁进行信息流交互的 VNF 易受到有害流的威胁和攻击。

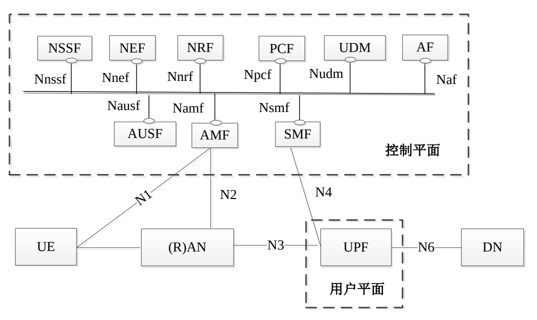


图 3 基于服务的 5G 网络架构

指标 3 根据 VNF 的度中心性。VNF 的度中心性是指网络拓扑中一个 VNF 与其他 VNF 直接相连接的数量。在 $Q^V=(F^V,E^V)$ 中，设 VNF 数量为 g 个，f_i^V 的度中心性计算为

$$C_D(f_i^V)=\sum_{j=1}^{g}x_{ij}(i\neq j) \tag{2}$$

其中：$\sum_{j=1}^{g}x_{ij}$ 表示为 f_i^V 与其他 $g-1$ 个 VNF 直接连接的数量[19]。由于用户不同的业务需求而使用不同的网络切片模板，导致网络切片内 VNF 的连接关系也有所不同，而 VNF 的度中心性能够直接反映网络切片内的 VNF 之间的连接关系。从受攻击后对整个网络的危害程度以及受攻击后恢复的难易程度上来说，度中心性越大的 VNF，其受攻击后对网络的影响更大且恢复也更为困难复杂。

指标 4 根据 VNF 资源需求。f_i^V 的资源需求表示为

$$Re(f_i^V)=\alpha\cdot C_i^V+\beta\cdot M_i^V \tag{3}$$

VNF 的资源需求是自身的能力因子，同时资源需求越高，其部署就越困难，因此资源需求高的 VNF 更加的重要，需要设定较高的安全等级来进行优先部署。α,β $(\alpha,\beta\in(0,1],\alpha+\beta=1)$ 是为消除由于量纲不同而导致的数值差异而设定的参数

指标 5 根据 VNF 的安全需求。VNF 的安全需求越高，表示对承载 VNF 的网络资源节点的安全信任值要求也越高，应考虑对其优先部署，防止由于和低安全 VNF 共享节点而可能导致的同驻攻击。

2.2 安全等级排序

在对网络切片中 VNF 安全等级进行分析排序时，若仅依靠某个计算指标来判断 VNF 的安全等级较为片面，若考虑多个指标，由于上述五种安全等级计算指标是从不同角度出发进行计算，指标结果可能会出现不一致的情况。为了综合多个计算指标，本文利用 TOPSIS 分析法将多个 VNF 安全等级计算指标转换为多属性决策排序。

TOPSIS(technique for order preference by similarity to ideal solution)分析法是一种逼近理想解的排序方法。TOPSIS 通过借助多属性问题中的理想解与负理想解，根据对评价对象的多个

属性与理想目标的接近程度进行排序。TOPSIS 排序方案的步骤如下：

步骤 1 建立安全等级决策矩阵 $X_{n\times m}$，如式(4)所示，假定网络切片中有 n 个 VNF，每个 VNF 有 m 个安全等级评价指标，x_{ij} 表示第 i 个 VNF 的 j 个安全等级评价指标。

$$X_{n\times m}=\begin{bmatrix} x_{11} & \cdots & x_{1j} & \cdots & x_{1m} \\ \cdots & & \cdots & & \cdots \\ x_{i1} & \cdots & x_{ij} & \cdots & x_{im} \\ \cdots & & \cdots & & \cdots \\ x_{n1} & \cdots & x_{nj} & \cdots & x_{nm} \end{bmatrix} \tag{4}$$

步骤 2 为消除量纲和量纲单位不同所带来的不可公度性，对决策矩阵进行规范化得到规范矩阵 $Z=\{z_{ij}\}$，其中 $z_{ij}=x_{ij}/\sqrt{\sum_{i=1}^{n}x_{ij}^2}$；同时设定加权矩阵 $\omega=(\omega_1,\omega_2,\ldots,\omega_m)^T$ 且 $\sum_{j=1}^{m}\omega_j=1$，得到加权规范矩阵 $Y=\{y_{ij}\}$，其 $y_{ij}=z_{ij}\cdot\omega_j, i=1,2,\ldots,n;\ j=1,2,\ldots,m$。

步骤 3 对于加权规范矩阵确定属性的理想解 y^* 和负理想解 y^o。

对于第 j 个属性的理想解为

$$y_j^*=\begin{cases}\max\limits_i y_{ij} \\ \min\limits_i y_{ij}\end{cases} i=1,2,\ldots,n,\ j=1,2,\ldots,m$$

对于第 j 个属性的负理想解为

$$y_j^o=\begin{cases}\max\limits_i y_{ij} \\ \min\limits_i y_{ij}\end{cases} i=1,2,\ldots,n,\ j=1,2,\ldots,m$$

步骤 4 计算各个安全等级评价指标与理想解和负理想解的欧氏距离。

对于第 i 个 VNF，其决策属性 y_{ij} 到理想解的欧氏距离 d_i^* 为

$$d_i^*=\sqrt{\sum_{j=1}^{m}(y_{ij}-y_j^*)^2}, i=1,2,\ldots,n \tag{5}$$

对于第 i 个 VNF，其决策属性 y_{ij} 到负理想解的欧氏距离 d_i^o 为

$$d_i^o=\sqrt{\sum_{j=1}^{m}(y_{ij}-y_j^o)^2}, i=1,2,\ldots,n \tag{6}$$

步骤 5 对各个 VNF 计算综合评价指数 C^*，第 i 个 VNF 的综合评价指数 C_i^* 为

$$C_i^*=\frac{d_i^o}{d_i^*+d_i^o}, i=1,2,\ldots,n \tag{7}$$

步骤 6 对的综合评价指数 C_i^* 的大小进行排序，C_i^* 越大，说明该 VNF 的安全等级越高。

3　网络切片部署算法设计

3.1　网络切片部署的数学模型

在对 VNF 部署方案进行分析评价时，主要以部署成本，安全收益和部署收益率作为部署方案的评价指标。

a) 对于一个网络切片部署请求 Q，其部署成本定义如下：

$$Cost(Q)=\sum_{f_i^V\in N^V}\sum_{n_j^P\in N^P}\rho(f_{i,j}^V)\bullet S_j^P\bullet(\alpha\cdot C_i^V+\beta\cdot M_i^V)+\sum_{e_{st}^V\in E^V}\sum_{e_{lv}^P\in E^P}\rho(e_{st,lv}^V)\bullet S_{lv}^P\bullet B_{st}^V\bullet Hop(e_{lv}^P) \tag{8}$$

其中：二元数值 $\rho\in\{0,1\}$ 作为决策变量来描述 VNF 和虚拟链路与底层网络资源之间的部署关系，ρ=1 表示成功部署，ρ=0 表示未部署成功。式(8)中第 1 项表示 VNF 部署成本，当 VNF 需要的 CPU 和存储资源越多，所部署的网络资源节点安全信任值越高，则 VNF 部署成本越高；第 2 项表示请求链路部署成本，当请求链路需要的带宽资源越多，部署的底层链路安全信任值越高，跳数越多，则请求链路部署成本越高。

b) 对于一个网络切片部署请求 Q，其安全收益定义如下：

$$Revenue(Q)=\sum_{f_i^V\in N^V}\sum_{n_j^P\in N^P}\rho(f_{i,j}^V)\bullet S_j\bullet(\alpha\cdot C_i^V+\beta\cdot M_i^V)+\sum_{e_{st}^V\in E^V}\sum_{e_{lv}^P\in E^P}\rho(e_{st,lv}^V)\bullet S_{lv}^P\bullet B_{st}^V \tag{9}$$

安全收益由部署占有的资源和整体的安全性所决定。由式(9)可知，网络切片部署时，所使用的底层网络资源越多，网络切片的整体安全性越高，安全收益也就越大。式(9)中第 1 项为 VNF 安全部署收益，S_j 表示承载 VNF 的网络资源节点 S_j^P 的综合安全性，由 VNF 安全和底层网络资源安全两部分组成，若只有一个 VNF 部署在 S_j^P 上，$S_j=S_i^V+S_j^P$；若有 r 个 VNF 部署在 S_j^P 上，$S_j=\min\{S_1^V,\ldots,S_r^V\}/r+S_j^P$，这是由于多个 VNF 部署在一个节点使得 VNF 相互攻击的安全风险成倍增加。第 2 项为请求链路部署的安全收益，其与所部署的底层链路的安全信任值以及所需链路带宽有关。

c) 对于一个网络切片部署请求 Q，其部署收益率定义如下：

$$\lambda=\frac{Revenue\ (Q)}{Cost\ (Q)} \tag{10}$$

部署收益率是对部署成本投入和安全收益产出的估算与衡量，由部署收益和部署成本所组成。由式(8)(9)可知，部署收益提高的同时会增大部署成本，在部署过程中，为追求部署效用的最大化，应尽可能控制部署成本并提高部署收益，而部署收益率越高，表明部署方案的效果越好。

3.2　优化目标和约束条件

优化目标：

$$\min\sum_{f_i^V\in N^V}\sum_{n_j^P\in N^P}\rho(f_{i,j}^V)\bullet S_j^P\bullet(\alpha\cdot C_i^V+\beta\cdot M_i^V)+\sum_{e_{st}^V\in E^V}\sum_{e_{lv}^P\in E^P}\rho(e_{st,lv}^V)\bullet S_{lv}^P\bullet B_{st}^V\bullet Hop(e_{lv}^P) \tag{11}$$

约束条件：

对于 $\forall f_i^V,f_k^V,f_s^V,f_t^V\in F^V$，$\forall n_j^P,n_l^P,n_v^P\in N^P$，$\forall e_{st}^V\in E^V$，$\forall e_{lv}^P\in E^P$，$\rho\in\{0,1\}$ 有

$$\begin{cases}\rho(f_{i,j}^V)\bullet R_i^V\le S_j^P \\ \rho(f_{i,j}^V)\bullet S_i^V\ge R_i^P \\ \rho(f_{i,j}^V)\bullet S_i^V\le\rho(f_{k,j}^V)\bullet S_k^V,\ f_i^V\text{先部署}\end{cases} \tag{12}$$

$$\rho(e^V_{st,lv})R^V_{st} \le S^P_{lv}\ (S^P_{lv} = \min_{\{e^P_{lo},\ldots,e^P_{rv}\}\in e^P_{lv}}\{S^P_l,\ldots,S^P_v\}) \tag{13}$$

$$\sum_{u=1}^{\sigma}\rho(f^V_{u,j})\bullet C^V_u \le C^P_j \tag{14}$$

$$\sum_{u=1}^{\sigma}\rho(f^V_{u,j})\bullet M^V_u \le M^P_j \tag{15}$$

$$\sum_{uw=1}^{\sigma}\rho(f^V_{uw,lv})\bullet B^V_{uw} \le B^P_{lv} \tag{16}$$

$$\sum_{f^V_i\in F^V}\rho(f^V_i)=1 \tag{17}$$

式(12)为上文提出的 VNF 部署时的安全约束条件 a)~c)，式(13)为链路部署的安全约束条件，式(14)~(16)是部署时对底层网络资源的约束条件。当网络切片部署时，式(14)(15)表示部署在同一底层网络资源节点的 VNF，其 CPU 和存储资源的需求和不能超过底层网络资源节点所能提供的资源能力，式(16)表示多条请求链路部署在同一条底层网络资源链路上，其带宽需求和不得超过底层网络带宽能力，式(17)表示一个 VNF 只能部署在一个底层网络资源节点上，不得拆分。

3.3　算法描述

本文提出一种启发式的安全部署算法命名为 NS-SD(network slice security deployment)，算法分为两个阶段：第 1 阶段对部署请求 Q^V 中每个 VNF 的安全等级评价指标进行计算并利用 TOPSIS 分析法对其安全等级进行排序；第 2 阶段针对优化目标进行求解。由于网络切片的部署策略模型是一个 NP 难问题，在底层网络资源无向图中运行隐枚举算法进行求解[20~22]，获取安全部署方案。

NS-SD 算法描述如下：

输入：网络切片部署请求无向图 Q^V；底层网络资源无向图 G^P。
输出：网络切片安全部署方案 NS_{sd}。
for 每一个 $f^V \in F^V$ do
　计算 f^V 的安全等级评价指标
end for
对于 n 个 VNF 建立安全等级决策矩阵 $X_{n\times 5}$，利用 TOPSIS 分析法对 VNF 的安全等级进行排序，排序结果存入链表 *SPList* 中
for *SPList* 中的每一个 VNF 和请求链路 do
　构建候选部署集合 $\Theta(f^V)$ 以及 $\Theta(e^V)$
end for
for $f^V_i\in\Theta(f^V)$ and $C^*_i \ge \forall C^*_x (i\ne x)$
　if n^P_j 未占用 and $\rho(f^V_{i,j})=1$ then
　n^P_j 不再部署其他 VNF and 部署结果放入 NS_{sd}
　else f^V_i 部署失败
　end if
end for
for $\Theta(f^V)=\{\Theta(f^V)\mid f^V_i\notin\Theta(f^V)\}$ and $\Theta(e^V)$ do
　隐枚举算法
　if 算法执行成功 then
　对底层网络资源进行更新 and 部署结果放入 NS_{sd}
　else 拒绝 $\Theta(f^V)$ and $\Theta(e^V)$
　end if
end for

算法(1)~(4)为算法的第 1 阶段，对 Q^V 中 VNF 的安全等级进行排序；(5)~(7)为部署准备，生成节点和链路集合；(8)~(20)为算法的第二阶段，其中(8)~(13)对安全等级最高的 VNF 进行优先部署，同时不共用底层节点，(14)~(20)表示对其他节点和链路利用整数线性规划算法进行部署，如果算法执行成功将输出部署方案 NS_{sd} 否则将拒绝部署。

4　仿真实验与分析

为了评价部署模型的可行性和 NS-SD 算法的有效性，本文根据部署成本、安全收益和成本收益率等方面进行仿真实验，并与其他算法进行比较并分析结果。

4.1　实验环境

针对底层网络资源拓扑图，为了保证拓扑图的随机性和不失一般性，本文利用机器学习中的 K 均值聚类算法生成无向图 G^P，共部署 80 个资源节点和相关链路[23]，如图 3 所示。

针对图 4 所生成的网络资源无向图，每个节点设置 CPU 能力 $C^P_x\in[5,30]$，存储能力 $M^P_x\in[10,100]$，安全信任值需求 $R^P_x\in(0,1]$ 和自身的安全信任值 $S^P_x\in(0,1]$ 等多个属性，每条链路设置带宽能力属性 $B^P_{xy}\in[1,20]$。

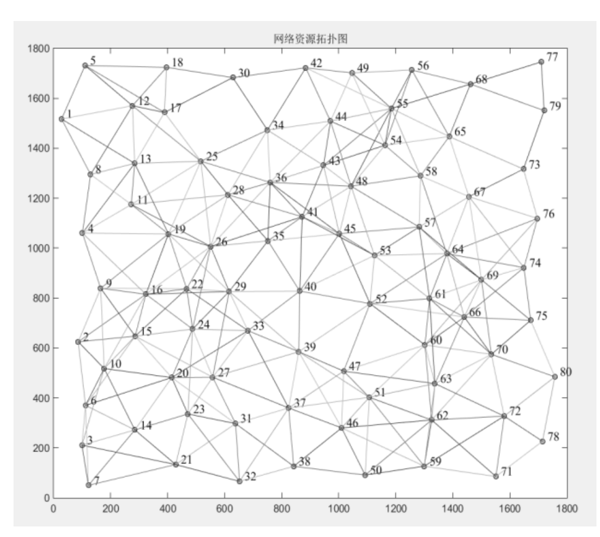


图 4　网络资源拓扑图

根据 3GPP 在 2017 年最新提出的技术规范 TS23.501[24]提到的 5G 网络架构，设计生成一个包含 15 个 VNF 的网络切片部署请求拓扑图，如图 5 所示。生成的拓扑图中，每个 VNF 随机设置 CPU 需求 $C^V_x\in[5,10]$，存储需求 $M^V_x\in[10,30]$，安全信任值需求 $R^V_x\in(0,1]$ 和自身的安全信任值 $S^V_x\in(0,1]$ 等多个属性，每条链路设置带宽需求属性 $B^V_{xy}\in[1,10]$，设定 α=0.7,β=0.3。随机设置 9 个控制平面 VNF，6 个用户平面 VNF，同时对每个 VNF 随机设置一个流量指标 T_i，TOPSIS 分析法中设置加权矩阵 ω 的元素均为 0.2。

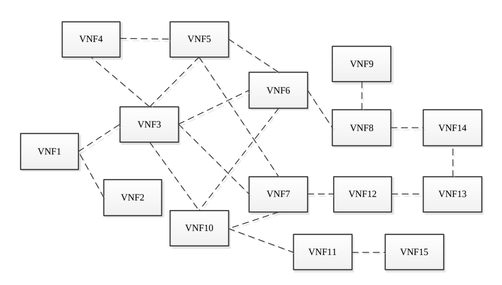


图 5　网络切片请求拓扑图

实验中，NS-SD 算法与其他三种算法进行比较，Greedy 算法是在切片部署阶段，根据 VNF 和请求链路的资源需求而采用的一种贪心部署策略[25]；MST 算法是基于最小生成树算法，通过考虑链路带宽资源需求和最小权重路径而采用的一种部署策略[26]；NNS-SD 是将 NS-SD 算法中的(8)~(13)步省略后的一种简化算法，在未考虑部分安全约束条件下来比较部署方案的收益与成本。为了使结果便于比较，Greedy 和 MST 算法在部署时加入新的安全部署约束。为避免随机性带来的影响，实验结果为多次实验后的平均值。

4.2　仿真结果分析

实验中以部署的成本，收益和收益率作为算法性能的评价指标，实验结果如下。

1）网络切片部署成本

图 6 为网络切片部署成本的变化情况。由图 6 可知，Greedy 算法在部署一开始，依靠选取最优的底层网络资源节点进行部署，实现 VNF 部署成本最小，但由于所选取的部署节点位置导致部分链路跳数过多而增大链路部署成本。MST 算法保证了链路部署成本最小，但 VNF 部署时由于选取部分底层网络资源节点的安全性过高而导致部署成本的增加。NS-SD 算法由于优先对高安全等级的 VNF 和链路进行部署，导致一开始部署成本增长较快，但隐枚举算法既考虑了链路跳数又尽可能在全局搜寻合适的网络资源节点和链路进行部署（节点和链路的安全信任值不会过高），随着 VNF 和请求链路部署的增加，使总的部署成本较低。NNS-SD 算法相比于 NS-SD 算法，其部署成本更低，主要是由于未考虑部分安全约束，使得部分 VNF 可以与最高安全等级的 VNF 共享底层资源，导致部署时降低了部分链路部署成本，但 NNS-SD 算法使得高安全等级的 VNF 受到同驻攻击的安全风险增大。实验表明，利用 NS-SD 算法，能够有效降低网络切片部署成本同时提高整个网络切片部署的安全性。

2）网络切片部署收益

图 7 为网络切片部署收益的变化情况。由图 7 可知，NS-SD 算法由于考虑了节点和链路全局的拓扑属性，在安全约束的前提下，在全局选取最合理的节点和链路进行部署，获得的部署总收益最高。Greedy 算法根据资源需求进行部署，对底层网络资源节点的安全性考虑较为局部，同时部署的节点和链路协调性较差，部署收益较低。MST 算法在部署一开始，根据其计算方法，使 VNF 能够部署在不同的网络资源节点上，尽可能减少 VNF 的网络资源节点共享情况，提高 VNF 的部署收益，但部署较为局部，全局考虑不足，导致整体的收益较低。NNS-SD 算法由于减少了安全约束条件，导致部分 VNF 资源共享，使部分 VNF 的安全部署收益相较于 NS-SD 算法较低。实验表明，NS-SD 算法在考虑安全约束下，有效提高了网络切片的部署收益。

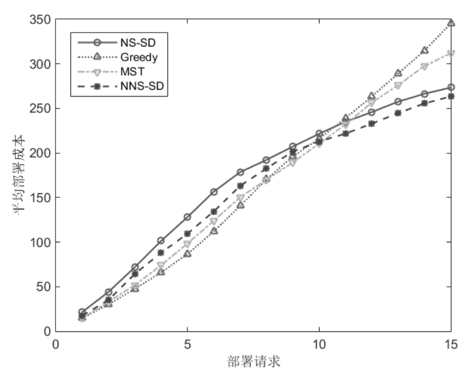


图 6　网络切片部署成本

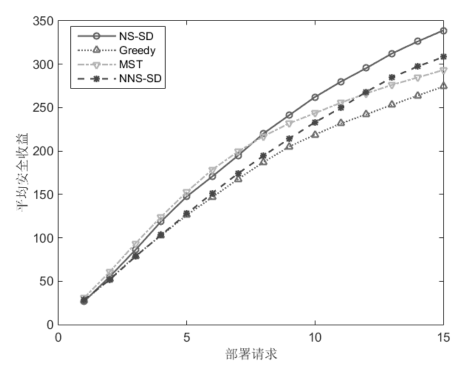


图 7　网络切片安全收益

3）网络切片部署成本收益率

图 8 为网络切片部署成本收益率的变化情况。如图 8 所示，NS-SD 和 NNS-SD 算法在部署一开始对高安全等级的 VNF 和请求链路进行部署，成本收益率较低，但部署过程中通过考虑全局的安全和资源属性，协调节点和链路部署，最终获得较好的部署成本收益率。Greedy 和 MST 算法在部署中对节点和链路协调较差，同时部署考虑较为局部，虽然在部署开始时可以获得较好的成本收益率，但整体部署方案的成本收益率随着 VNF 和请求链路部署增加而降低。实验表明，NS-SD 算法得到的部署方案，在保证安全性的前提下，通过分析底层网络资源的全局属性，协调节点和链路进行部署，有效提高整体的成本收益率。

5　结束语

5G 网络切片由于采用虚拟化技术而引入了新的安全问题，本文主要研究了在虚拟化环境下的网络切片部署问题，针对现有网络切片部署方法的不足和网络切片高安全性需求，提出一种基于安全信任的网络切片部署策略，并通过仿真实验验证了

部署模型的可行性和算法的有效性。该方法通过对 VNF 以及网络资源安全性的量化和对 VNF 安全等级的排序，实现对网络切片中高安全等级的 VNF 进行重点保护。仿真实验结果表明，本文提出的部署策略，在保证安全的前提下，能够选取合适的节点和链路进行网络切片的部署，有效降低部署成本，同时获得较好的安全收益和部署收益率。在后续研究中，针对网络切片商用运行过程中可能出现的安全问题进行研究，以保证网络切片的高安全性需求。

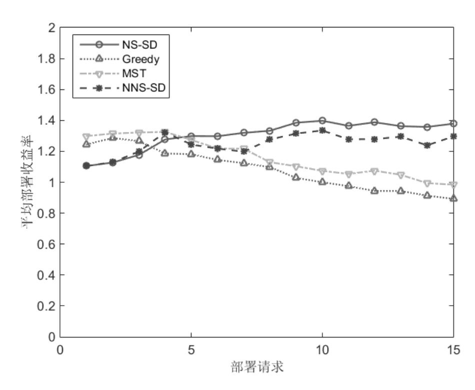


图 8　网络切片部署成本收益率

参考文献：

[1] China Mobile Communications Corporation. 5G service-guaranteed network slicing new white paper [EB/OL]. (2017-03-01) [2017-05-20]. http://www. huawei. com/ch-en/news/ch/2016/5G.

[2] 陈山枝. 发展 5G 的分析与建议 [J]. 电信科学, 2016, 32 (7): 1-10.

[3] Fischer A, De Meer H. Position paper: secure virtual network embedding [J]. Praxis der Informationsverarbeitung und Kommunikation, 2011, 34 (4): 190-193.

[4] Aljuhani A, Alharbi T. Virtualized network functions security attacks and vulnerabilities [C]// Proc of the 7th Annual Computing and Communication Workshop and Conference. 2017: 1-4.

[5] 汤红波, 袁泉, 卢干强, 等. 一种支持节点分割的 vEPC 虚拟网络功能部署模型 [J]. 电子与信息学报, 2017, 39 (3): 546-553.

[6] Baumgartner A, Reddy V S, Bauschert T. Mobile core network virtualization: a model for combined virtual core network function placement and topology optimization [C]// Proc of IEEE Network Softwarization. 2015: 1-9.

[7] Otokura M, Leibnitz K, Koizumi Y, et al. Application of evolutionary mechanism to dynamic Virtual Network Function Placement [C]// Proc of IEEE Workshop Coolsdn. 2016: 1-6.

[8] Cao J, Zhang Y, Wei A, et al. VNF-FG design and VNF placement for 5G mobile networks [J]. Science China Information Sciences, 2017, 60 (4): 040302.

[9] Cohen R, Lewin-Eytan L, Naor J S, et al. Near optimal placement of virtual network functions [C]// Proc of IEEE Computer Communications, 2015: 1346-1354.

[10] Luizelli M C, Bays L R, Buriol L S, et al. Piecing together the NFV provisioning puzzle: efficient placement and chaining of virtual network functions [C]// Proc of IFIP//IEEE International Symposium on Integrated Network Management. 2015: 98-106.

[11] Moens H, Turck F D. VNF-P: a model for efficient placement of virtualized network functions [C]// Proc of IEEE International Conference on Network and Service Management. 2014: 418-423.

[12] Luizelli M C, Cordeiro W L D C, Buriol L S, et al. A fix-and-optimize approach for efficient and large scale virtual network function placement and chaining [J]. Computer Communications, 2016, 10 (2): 67-77.

[13] Ghaznavi M, Khan A, Shahriar N, et al. Elastic virtual network function placement [C]// Proc of the 4th International Conference on Cloud Networking. 2015: 255-260.

[14] Ravindran R, Chakraborti A, Amin S O, et al. 5G-ICN: delivering ICN services over 5G using network slicing [J]. IEEE Communications Magazine, 2017, 55 (5): 101-107.

[15] Zhou X, Li R, Chen T, et al. Network slicing as a service: enabling enterprises'own software-defined cellular networks [J]. IEEE Communications Magazine, 2016, 54 (7): 146-153.

[16] Nikaein N, Schiller E, Favraud R, et al. Network store: exploring slicing in future 5G networks [C]// Proc of International Workshop on Mobility in the Evolving Internet Architecture. 2015: 8-13.

[17] 汪京培, 孙斌, 钮心忻, 等. 基于可信建模过程的信任模型评估算法 [J]. 清华大学学报: 自然科学版, 2013, 53 (12): 1699-1707.

[18] 孟顺梅. 云计算环境下可信服务组合及其关键技术研究 [D]. 南京: 南京大学, 2016.

[19] Stanley W, Katherine F. Social network analysis: methods and applications [M]. Beijing: China People's University Press, 2012: 42-64.

[20] Shao W, Hu W, Huang X. A new implicit enumeration method for linear 0-1 programming [C]// Proc of IEEE International Workshop on Modelling, Simulation and Optimization. 2008: 298-301.

[21] Geoffrion A M. An improved implicit enumeration approach for integer programming [J]. Operations Research, 1969, 17 (3): 437-454.

[22] Wang Jun, Li Duan. A new implicit enumeration method for polynomial 0-1 programming and applications [J]. System Engineering Theory and Practice, 2007, 27 (3): 21-27.

[23] Harrington P. Machine learning in action [M]. Beijing: The People's Posts and Telecommunications Press, 2013: 15-31.

[24] 3GPP. TR23. 501, 3rd generation partnership project; technical specification group services and system aspects; procedures for the 5G system; rel. 15 [EB/OL]. (2017-04) [2017-05-20]. http://www. 3gpp. org/ftp/Specs/latest-drafts/.

[25] Yu M, Yi Y, Rexford J, et al. Rethinking virtual network embedding: substrate support for path splitting and migration [J]. ACM Sigcomm Computer Communication Review, 2008, 38 (2): 17-29.

[26] 彭利民. 基于最小代价的跨域虚拟网络映射算法 [J]. 华南理工大学学报: 自然科学版, 2015, 43 (9): 67-73.